Section 8

SUPPORT SYSTEMS

Contents

References

DOE Order 5632.1C

General Information

Although not an independent subtopic of PSSs, support systems include a number of interrelated subjects of interest to inspectors examining this topic. Although normally inspected along with the traditional subtopics, these subjects merit separate discussion to ensure they are adequately addressed during the inspection process. They include power supplies, tamper protection, and regulatory warning signs.

For the purposes of security systems, auxiliary power is defined as an uninterruptible power supply or a power supply provided by engine-driven generators. In the event that the primary power source fails, DOE requires that transfer to auxiliary power must be automatic without affecting the security system or device being protected. Both the CAS and the SAS must receive an alarm indicating failure of any power source and transfer to auxiliary power. Auxiliary power supply configurations vary widely throughout the DOE complex depending upon the system, the equipment, and the manufacturer.

The reason for evaluating auxiliary power supplies is to determine whether they are adequate to power all alarm systems and critical equipment for a sufficient time to permit restoration of normal power.

Batteries are also a means of auxiliary power, and there are a number of provisions related to their use. When rechargeable batteries are used, they should be kept fully charged or subject to automatic recharging whenever the voltage drops to a specified level. Non-rechargeable batteries should be replaced whenever their voltage drops 20 percent below the rated voltage. An alarm signal should be activated to indicate this condition.

There are various methods to prevent and detect attempts to tamper with security systems. Tamper protection is covered in detail in Appendix D, which provides information for testing of components used to indicate that detection devices or transmission lines to annunciators have failed or been tampered with. If operational or process control information (for example, low rates, pressure readings, or airborne radiation levels) is relied on for security purposes, these systems should be checked for tamper resistance.

Tamper and line supervision tests are usually conducted in conjunction with related tests of CCTV equipment and the intrusion-detection and access-control systems to increase the efficiency of data gathering.

The posting of signs listing regulations and penalties is provided for by the Atomic Energy Act of 1954. Typically, these signs list prohibited activities, such as unauthorized entry onto DOE property, and the fines or imprisonment violators may receive if convicted. Signs are normally posted at entrances and at intervals along the

perimeter of the property. Signs posted at entrances normally list prohibited articles, such as firearms, explosives, privately owned recording and electronic equipment, cellular telephones, computers, controlled substances, and others. Notification of the date of posting, relocation, or removal of posting, or other changes should be furnished to the local office of the FBI exercising investigative responsibility over the property.

Common Deficiencies/ Potential Concerns

Often, supporting devices associated with auxiliary power sources are not afforded adequate tamper protection. These items may include batteries, inverters, power switches, and fuel supplies. When one or more of these items are disabled, the auxiliary power source may be effectively neutralized. For example, if the fuel tank that furnishes fuel for a generator—the primary backup power source for a particular security system—is contaminated or destroyed, the backup power source is effectively eliminated, although the generator itself may be adequately protected.

Since batteries can be hazardous (battery acid can burn or be extremely corrosive, and batteries do occasionally explode), routine servicing and testing is important. Sometimes, inspectors will find batteries left unattended and in poor condition. Some associated problems can be identified early in the inspection by checking testing and maintenance procedures.

The most significant concern in the area of tamper protection is the frequent failure by DOE facilities to provide complete tamper indication and line supervision for all security system elements and devices requiring protection. This includes tamper devices such as magnetic switches, plungers, and closure contacts. These devices should be inaccessible, located inside a protected space, or otherwise protected.

Frequently, line supervision fails to include the entire circuit to be protected (that is, the sensor itself, local wiring to a control device, the transmission medium, and the final signal processing annunciation equipment). In this event, the destruction or failure of the unprotected component could result in the failure of the whole system.

In some cases, multiple tamper devices are included on a single alarm circuit to reduce wiring and signal processing requirements. This can be a significant weakness since the actual type and location of the alarm, and the number of affected devices, may not be apparent from the information displayed at the alarm console.

Planning Activities

Inspectors review documentation and interview facility representatives to gather information on auxiliary systems, including power supplies and tamper alarms. If vital or security-related equipment relies on cooling water (for example, reactor coolant pumps) or fuel supplies (for example, engine generators) inspectors should determine methods used by the facility to ensure the reliability of such systems.

Performance Tests

All performance tests cited in the appendices may be relevant to assessment of support systems, especially those pertaining to auxiliary power supplies and tamper alarms (Appendix D).

Data-Collection Activities

Power Supplies

A. Inspectors should interview security staff and review documents to determine:

- What security-related components are supplied auxiliary power by batteries, an uninterruptible power source (UPS), or other means
- Length of time that the UPS will maintain operation at full load and procedures for load shedding
- Number and location of diesel generators

- Security-related components that are supplied auxiliary power by engine generators
- Length of time that diesel generators will maintain load until fuel supply is exhausted
- Frequency and methods for testing and maintaining diesel generators (for example, full load tests, test of switching devices)
- Frequency and methods for testing and maintaining system batteries or the UPS
- Frequency and methods for testing and maintaining batteries that power individual components (for example, sensors)
- Replacement frequency for non-rechargeable batteries
- Indications received in CAS/SAS when normal or auxiliary power fails
- Source of offsite electric power, including number of feeds
- How the systems are tested (are they turned on, brought up to speed and then is the load switched, or does the test actually simulate power loss?).

B. Inspectors should tour areas where components critical to providing auxiliary power are located and verify information gathered during document reviews and interviews. Items of interest include fuel supply reservoirs, switching equipment, batteries and power-generating equipment. All of these elements should be given adequate physical protection, including tamper protection and shielding from inclement weather. For example, the switching equipment for the commercial to auxiliary power transfer should not be installed on the outside of a security area where access is unrestricted and the opportunity for undetected tampering could occur.

Tamper Protection

C. Inspectors should review the methods to prevent and detect attempts to tamper with security-related systems, including the use and inspection frequency of tamper-resistant hardware and tamper indicating devices (TIDs). Also, inspectors should review the general installation techniques for security sensors (that is, the use of epoxy over screws or bolts, security seals, or deformation of threads on attachment hardware). If operational or process information is used for security purposes, this equipment should have many of the same physical protection features as security equipment. The use of TIDs and security hardware should also be reviewed, to include the level of confidence or response placed on this type of alarm (that is, does the protective force initiate a full-blown response or is an SPO dispatched to investigate the alarm?).

Signs

D. Inspectors should check signs to determine whether the required signs are appropriately placed and in good repair as required by the DOE orders and site security plans. Warning signs concerning the use of deadly force, vehicle and personnel searches, and contraband searches are normally posted at entrances to security areas.

This page is intentionally left blank.